PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	Make **2-3 notes** of specific business requirements that will be analyzed. ● *Will the app process transactions?* ○ *Yes, it will directly connect buyers and sellers and handle transactions.* ● *Does it do a lot of back-end processing?* ○ *Yes, it needs to securely store and transfer payment data between users. Data privacy is essential.* ● *Are there industry regulations that need to be considered?* ○ *Yes, the app must comply with industry regulations such as PCI-DSS and local data protection laws.*
II. Define the technical scope	List of technologies used by the application: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *SHA-256* ● *SQL* Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others. - I prioritized public key infrastructure, SHA-256, and SQL because the application handles sensitive user data and payment information. Ensuring data confidentiality, integrity, and secure storage is critical for a shoe-selling business that processes online transactions.
III. Decompose application	Sample data flow diagram A man-in-the-middle (MitM) attack could compromise the data flow by impersonating the product search process. An attacker could trick users into submitting personal or payment data to a fake sneaker database, collecting sensitive information under the guise of showing product listings.

IV. Threat analysis	List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application. ● *What are the internal threats?* ○ *Weak PKI practices, such as users creating common or reused passwords, can lead to credential theft.* ○ *Malware or viruses targeting the authentication module may compromise login security.* ● *What are the external threats?* ○ *A man-in-the-middle (MitM) attack could intercept communication between the user and the server.* ○ *A threat actor posing as an employee may install malware through social engineering or phishing tactics.*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *Could there be things wrong with the codebase?* ○ *The application does not enforce two-factor authentication, which increases the risk of unauthorized access during online transactions.* ● *Could there be weaknesses in the database?* ○ *The system is vulnerable to SQL injection, allowing a threat actor to bypass login or manipulate sneaker purchase records without payment.* ● *Could there be flaws in the network?* ○ *The database may be exposed to man-in-the-middle (MitM) attacks, where attackers intercept traffic and collect user credentials or financial information.*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	List **4 security controls** that you've learned about that can reduce risk. 1. Enforce strong password policies to reduce unauthorized access risk. 2. Use SHA-256 and SFTP protocols to securely store and transmit user data, including credit card and database information. 3. Implement two-factor authentication (2FA) for all user

	transactions to verify identity. 4. Regularly update the application and patch known vulnerabilities to prevent exploitation by emerging threats.